(19) (11) Publication number: **10240517 A**

Generated Document.

PATENT ABSTRACTS OF JAPAN

(21) Application number: **09038173** (51) Intl. Cl.: **G06F 9/06**

(22) Application date: **21.02.97**

(30) Priority:

(43) Date of application publication: **11.09.98**

(84) Designated contracting states:

(71) Applicant: **SONY CORP**

(72) Inventor: **WATANABE HIDEKAZU**

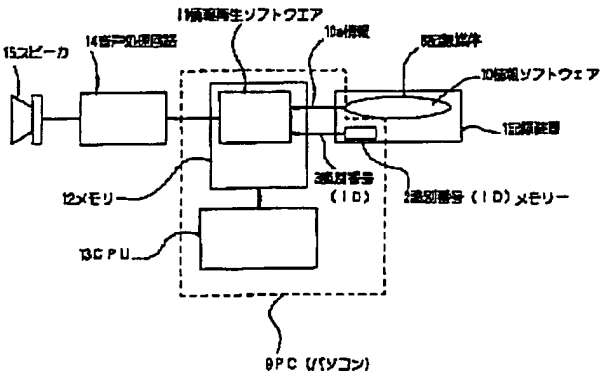
(74) Representative:

(54) METHOD AND DEVICE FOR PREVENTING DUPLICATION OF SOFTWARE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a method and a device for preventing the duplication of a software capable of preventing the software loadable to a computer from being easily copied.

SOLUTION: An identification number(ID) 3 is attached to a recorder 1 capable of preserving the software and the software is provided with a program for inspecting the identification number. At the time of reading the software into the computer 9, the identification number 3 is inspected by the program for inspecting the identification number provided in the software, and when the identification number 3 satisfies inspection conditions, the reproduction of the software is made possible and the duplication of the software is prevented.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－240517

(43)公開日　平成10年(1998)９月11日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｆ　9/06	５５０	Ｇ０６Ｆ　9/06	５５０Ｈ

審査請求　未請求　請求項の数13　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－38173

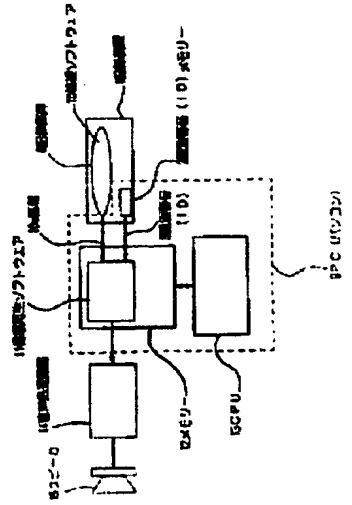
(22)出願日　平成９年(1997)２月21日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　渡辺　秀和
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(54)【発明の名称】　ソフトウェアの複製防止方法及び装置

(57)【要約】
【課題】　コンピュータにロードできるソフトウェアを容易にコピーすることを防止できるソフトウェアの複製防止方法及び装置を提供する。
【解決手段】　ソフトウェアを保存することのできる記録装置１に、識別番号（ＩＤ）３を付し、前記ソフトウェアに前記識別番号の検査用プログラム を含め、前記ソフトウェアをコンピュータ９内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラム により前記識別番号３を検査し、前記識別番号３が検査条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。



【特許請求の範囲】
【請求項 1】　ソフトウェアを保存することのできる記録装置に、識別番号を付し、
前記ソフトウェアに前記識別番号の検査用プログラム を含め、
前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、
前記識別番号が検査条件を満たした際、
前記ソフトウェアの再生を可能としたことを特徴とするソフトウェアの複製防止方法。
【請求項 2】　前記記録装置が記録媒体であ ることを特徴とする請求項 1に記載のソフトウェアの複製防止方法.
【請求項 3】　識別番号を付した記録装置と、
検査用プログラム を含むソフトウェアとを具備し、
前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、
前記識別番号が検査条件を満たした際、
前記ソフトウェアの再生を可能としたことを特徴とするソフトウェアの複製防止装置。
【請求項 4】　前記記録装置が記録媒体であ ることを特徴とする請求項 3に記載のソフトウェアの複製防止装置。
【請求項 5】　ソフトウェアにコンピュータに付した識別番号に対応したデータを組み込み、
前記コンピュータに前記ソフトウェアに含む識別番号検査用プログラム をロードし、
前記ソフトウェアの利用時に、前記識別番号検査用プログラム により、
コンピュータの識別番号と前記ソフトウェアに組み込んだデータとの一致性を検査することを特徴とするソフトウェアの複製防止方法。
【請求項 6】　ソフトウェアに識別番号を用いた暗号化処理を行うステップと、
前記暗号化されたソフトウェアを記録装置に保存するステップと、
前記ソフトウェアの再生ソフトウェアをコンピュータのメモリーに読み出すステップと、
前記記録装置又は記録媒体に記憶され暗号化された識別番号を読み出すステップと、
前記記録媒体から識別番号から成る鍵番号を読み出すステップと、
前記識別番号の復号化ソフトウェアによって前記鍵番号と暗号化された識別番号から識別番号を復号化するステップと、
前記復号化された識別番号を用いて前記再生ソフトウェアでソフトウェアを再生するステップを含むことを特徴とするソフトウェアの複製防止方法。
【請求項 7】　記録装置に暗号化されたソフトウェアを復号化する復号手段及び識別番号メモリーを備え、
ソフトウェアの再生ソフトウェアと動作指示プログラムがロードされたコンピュータのメモリーを備え、
前記識別番号メモリーから読み出された識別番号により前記動作指示プログラム により前記復号手段にコマンドを与え、前記復号手段で前記ソフトウェアを復号化し、
前記再生ソフトウェアによりソフトウェアを再生することを特徴とするソフトウェアの複製防止装置。
【請求項 8】　通信ネットワークを通じて、所望のソフトウェアを注文する際、記録装置等に付された識別番号を送信するステップと、
受信側では注文された前記ソフトウェアに前記識別番号から付加情報を付加して転送するステップを含むことを特徴とするソフトウェアの複製防止方法。
【請求項 9】　保存されたソフトウェアを利用をする際に、利用者に個別に割り当てられた、利用者番号も合わせて検査することを特徴とする請求項 1又は請求項 6に記載のソフトウェアの複製防止方法。
【請求項 10】　ソフトウェアを保存することのできる記録装置に識別番号を記憶した識別番号記録メモリーを備えたことを特徴とする記録装置。
【請求項 11】　ソフトウェアを保存することのできる記録媒体に識別番号を記憶させたことを特徴とする記録媒体。
【請求項 12】　前記ソフトウェアがプログラム ソフトウェアであ ることを特徴とする請求項 1又は請求項 2又は請求項 5又は請求項 6又は請求項 8又は請求項 9に記載のソフトウェアの複製防止方法。
【請求項 13】　前記ソフトウェアがプログラム ソフトウェアであ ることを特徴とする請求項 3又は請求項 4又は請求項 7に記載のソフトウェアの複製防止装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
【０００２】本発明はパーソナルコンピュータ等にロードするソフトウェアの不正な複製を防止するソフトウェアの複製防止方法及び装置に関する。
【０００３】
【従来の技術】最近ではパソコン通信や、インターネット接続を行っての通信が様々な形で行われており、様々なコンピュータデータやプログラム 等のソフトウェアが、ディジタルデータとして流通しており、それがハードディスク装置などの記録媒体に最初は代金を支払って合法的に記録された場合でも、その後はダウンロードしたソフトウェアは容易にコピー（複製）可能であ る。しかも、コピーしたデータはディジタルデータのため、元のものとまったく同一内容であ り、これらを区別することはできない。
【０００４】従って、このようなディジタルデータは、

何回もコピーを取られたり、不正利用されやすかった。
ＰＣのプログラム などのソフトウェアはプログラム 自体にプログラム の有効期限を設定することができるので、それを利用してプログラム の長期不正利用を防ぐことができるが、音楽や絵のデータなどの各種ディジタルデータはプログラム のように有効期限を付けることも難しく、余り有効な複製防止手段がなかった。
【０００５】ここで述べるソフトウェアとしては、ＰＣ（パソコン）等で取り扱うことが可能な各種ディジタルデータ、音楽データ、画像データなど広義のディジタルデータである。最近のＰＣは大容量のハードディスク（以下ＨＤと略す）を備え、そこへ各種ソフトウェアを置き、必要に応じてそれをＰＣ上の処理ソフトウェアを利用し使うことが一般的になっている。
【０００６】コピーされたデータはフロッピーディスク（以下ＦＤと略す）や通信回線を通じ他のＰＣに自由に移植可能であり、これは元のデータを作った者の著作権を無視した不正利用の根源にもなっている。このためソフトウェアの不正利用を防止することは、ソフトウェアを配布する上では、大きな課題となっている。
【０００７】特に近年では、インターネットや、パソコン通信などのコンピュータネットワークを通じて、ソフトウェアを配布することが一般的に行われるようになってきているので、そのようなソフトウェアの不正使用を防止することは急務になってきている。このようなソフトウェアの場合、利用者がソフトウェアを購入するにも店舗に行く必要はなく、ネットワークを通じて必要なものを入手できるため、大変便利であるが、一方ソフトウェアを販売する側としては、ＰＣなどで簡単に複製可能なディジタルデータをネットワークで伝送することは、データの不正コピーが作りやすいという点で、大きな問題となる。
【０００８】又はこれとは別に、記録メディアの進歩により、従来より使われていたＨＤ，ＦＤ，磁気テープなどとは別にＭＯ，ＰＤ，ＺＩＰ，媒体交換可能型ＨＤ，ＤｅｔａＭＤなど多くの種類の大容量記録媒体が開発され、しかもこれらのものは記録媒体のみを携帯して持ち運ぶことも可能である。これらの記録媒体を使用すれば、異なるＰＣ間でデータをコピーし交換することも容易である。従って、これも又はソフトウェアの不正使用の点では、問題である。
【０００９】しかしコンピュータのユーザーにとっては、これらの記録媒体を使用することで簡単にソフトウェアを持ち運んだり、バックアップを取ったりすることができるため、これらの使用を禁止することは現実的ではない。従って、このような記録媒体を今迄どおりに使用しながら、ソフトウェアの不正使用を防止する技術が強く求められている。
【００１０】本発明はそのような技術の一つであり、記録媒体又は記録装置に、利用者からは書換え困難なユニークな番号を書き込んでおくことにより、ソフトウェアの不正使用を防ぐためのものである。
【００１１】これらの記録装置は図１１に示すように、ディスクトップ型のＰＣ（パーソナルコンピュータ）９の場合にはＳＣＳＩと呼ばれる周辺機器インターフェースを利用してＰＣ９と記録装置１が接続されることが多い。そしてＦＤ，ＭＯ，ＰＤといった記録媒体８は、それを動作させるための機器（ドライブ）と記録媒体８そのもの（メディア）を分離することができ、必要なときに必要な記録媒体８をそれを使うための機器に挿入することで、自由にソフトウェアの読み出、書き込みができるようになっている。
【００１２】又は、ＳＣＳＩを用いて外付のＨＤを接続することも可能である。このようなＨＤの場合、通常は記録媒体８を記録装置から分離することはできない。又はノート型ＰＣなどの携帯型端末では、図１２に示すごとく、端末のインターフェースとしてＰＣＭＣＩＡインターフェースと呼ばれるものを持ち、これを使用して外部機器とＰＣ９を接続できるようになったものが、最近は多くなっている。ＰＣＭＣＩＡインターフェースはカード型のインターフェースカードをＰＣ９本体に挿入して使うことができ、小型機器のインターフェースとしては使いやすいものである。
【００１３】ＰＣＭＣＩＡインターフェースカードは、もともとはメモリーカードが出発点であり、メモリーカードとして様々なデータを記憶できるものもあるが、現在ではメモリーカードだけではなく様々な種類のものがあり、上述のＳＣＳＩインターフェース用のカードなどもある。ＳＣＳＩインターフェース用のＰＣＭＣＩＡカードを使用したときには、ＳＣＳＩを利用し、ＰＣ９と外部装置を接続することも可能である。
【００１４】又は、ＰＣＭＣＩＡカードの中にはそれ自体がハードディスク装置になっているものもあり、その場合には図１２に示すように、ＰＣＭＣＩＡカード型ＨＤ装置（記録装置１）をＰＣ９に接続するだけで、データの読み書きができるようになる。従って、この場合にはＰＣＭＣＩＡ型ＨＤ装置自体を、ＦＤのように自由に持ち運んで使用することもできる。
【００１５】本発明はこのような記録媒体を用いて、音楽データや画像データといったソフトウェアを利用するときにその不正使用を防止するためのものである。このような記録媒体にあるソフトウェアを記憶して利用するとき、上述のようにＰＣでは通常簡単にデータファイルのコピーができるので、記録されたソフトウェアを不正にコピーしそれをＰＣ内部のＨＤに移して利用するようなことは難しくない。
【００１６】それを防止するために、本発明では記録媒体又は記録装置にユニークなナンバーから成る識別番号（ＩＤ）を付け、そのＩＤを利用し、ＨＤに記録するソフトウェアの検査を行い、不正コピーの防止を行うもの

である。ＩＤは記録媒体に記録しても良いし、それを操作するための記録装置自体に記憶しても良い。通常のＨＤの様に記録媒体と記録装置が一体化されたものもどちらにＩＤが書き込まれていても問題はないが、記録装置にハードウェア的に書き込まれていたほうが、ＩＤを簡単には書換えできず安全性の点で扱いやすい。

【００１７】

【発明が解決しようとする課題】本発明はコンピュータにロードできるソフトウェアをコピーすることを防止できるソフトウェアの複製防止方法及び装置を提供することを目的とする。

【００１８】

【課題を解決するための手段】請求項１に係る本発明のソフトウェアの複製防止方法は、ソフトウェアを保存することのできる記録装置に、識別番号（ＩＤ）を付し、前記ソフトウェアに前記識別番号の検査用プログラムを含め、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。

【００１９】請求項２に係る本発明のソフトウェアの複製防止装置は、識別番号を付した記録装置と、検査用プログラムを含むソフトウェアとを具備し、前記ソフトウェアをコンピュータ内に読み出す際、前記ソフトウェアに含んだ前記識別番号の検査用プログラムにより前記識別番号を検査し、前記識別番号が検査条件を満たした際、前記ソフトウェアの再生を可能とし、ソフトウェアの複製を防止する。

【００２０】請求項３に係るソフトウェアの複製防止方法は、ソフトウェアにコンピュータに付した識別番号に対応したデータを組み込み、前記コンピュータに前記ソフトウェアに含む識別番号検査用プログラムをロードし、前記ソフトウェアの利用時に、前記識別番号検査用プログラムにより、コンピュータの識別番号と前記ソフトウェアに組み込んだデータとの一致性を検査し、ソフトウェアの複製を防止する。

【００２１】請求項４に係る本発明のソフトウェアの複製防止方法は、ソフトウェアに識別番号を用いた暗号化処理を行うステップと、前記暗号化されたソフトウェアを記録装置に保存するステップと、前記ソフトウェアの再生ソフトウェアをコンピュータのメモリーに読み出すステップと、前記記録装置又は記録媒体に記録され暗号化された識別番号を読み出すステップと、前記記録媒体から識別番号から成る暗番号を読み出すステップと、前記識別番号の復号化ソフトウェアによって前記暗番号と暗号化された識別番号から識別番号を復号化するステップと、前記復号化された識別番号を用いて前記再生ソフトウェアでソフトウェアを再生するステップを含むソフトウェアの複製を防止する。

【００２２】請求項７に係るソフトウェアの複製防止装置は、記録装置に暗号化されたソフトウェアを復号化する復号手段（復号用ハードウェア）及び識別番号記録メモリー（ＩＤメモリー）を備え、ソフトウェアの再生ソフトウェアと動作指示プログラムがロードされたコンピュータのメモリーを備え、前記識別番号記録メモリーから読み出された識別番号により前記動作指示プログラムにより前記復号手段にコマンドを与え、前記復号手段で前記ソフトウェアを復号化し、前記再生ソフトウェアによりソフトウェアを再生し、ソフトウェアの複製を防止する。

【００２３】請求項１０に係る記録装置はソフトウェアを保存することのできる記録装置に識別番号を記録した識別番号記録メモリー（ＩＤメモリー）を備えた構成とし、ソフトウェアの複製を防止する。

【００２４】

【発明の実施の形態】以下に本発明の好適な実施の形態について、図面を参照しつつ詳細に説明する。

第１の実施の形態

このような識別番号（ＩＤ）は利用者によって簡単には書換えられないように、設定されている必要があり、図１に示すように記録装置１内部のＲＯＭ２（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）などに識別番号（ＩＤ）３がハードウェア的に書かれていれば、書換えに対する安全性は高い。

【００２５】記録装置１は例えばハードディスク駆動装置であり、制御回路４にＲＯＭ２、書込回路５、読込回路６、Ｉ／Ｆ（インターフェース回路）７を接続し、図示しない機構部にセットされた記録媒体（例えばハードディスク）８にデータを書き込んだり、読み出す。又は、図示しないパソコン９との間で、これらのデータを１／Ｆ７を介してやりとりする構成となっている。

【００２６】第２の実施の形態

記録媒体にＩＤが書き込まれる場合にも、通常は利用者によって書換えることのできない記録媒体の領域、例えば図２に示すように記録媒体（ハードディスク）８全体の状態を制御するための領域（管理データ領域９ｂ）や、通常では使うことのない記録媒体上のデータ領域間の隙間などに識別番号（ＩＤ）３を書き込むことにし、一般の利用者はＩＤ３を簡単には書換えることができないようにしておく。

【００２７】尚、管理データ領域９ｂはセクター９ａで区切られた領域に分けられている。このようなしておかないと不正利用者にＩＤを書換えられソフトウェアの不正コピーをされてしまう恐れもある。以下に、このようなＩＤを用いて、どのようにソフトウェアの不正利用を防ぐのか説明する。ここでは記録媒体としてハードディスク（ＨＤ）、記録装置としてハードディスク駆動装置を想定して説明を行うが、他の記録媒体と駆動装置でも、まったく同様である。

【００２８】第３の実施の形態
この第１の方法は、記録されているディジタルデータの使用時に、記録装置又は記録媒体に書かれているＩＤを直接チェックすることで、不正利用防止を行う方法である。図３は音楽が記録されたデータ（情報ソフトウェア１０）を、ＰＣ（パソコン）９を使い音楽を聴くための機能ブロック図であり、ＰＣ９に記録装置１の記録媒体８から音楽等の情報１０ａを供給し、又は再生に当たりメモリー１２に置いた情報再生ソフトウェア１１を用いて音楽を再生する。
【００２９】情報再生ソフトウェア１１にて再生される音楽情報はＤ／Ａ変換器、増幅器等を含む音声処理回路１４からスピーカ１５に至り、音声として出力される。これらの処理はＣＰＵ１３の制御の下に実行される。そして、この場合は記録装置１にＲＯＭからなる識別番号（ＩＤ）メモリー２が備えられ、ＩＤメモリー２には記録装置１毎に個別のＩＤ３が付されている。情報再生ソフトウェア１１はプラグイン式のものが一般的であり、通信手段やＣＤ－ＲＯＭ等から、ハードディスク等の記録媒体８にロードされる。
【００３０】そして、音楽再生のための情報再生ソフトウェア１１にＩＤチェックのためのプログラム を予め組み込んでおき、再生時に、このプログラム を用いてＩＤメモリー２に含まれたＩＤ３をチェックし、それが正当なものであれば再生を実行し、ＩＤが不当な場合には再生を実行しないようにして、ソフトウェアの不正利用防止を図たす。
【００３１】尚、この場合はＩＤ３を記録装置１に設けたＩＤメモリー２に付したが、内蔵 ハードディスク等の記録媒体８の管理領域に付しても同等である。又は、ＩＤのチェックに際しては、再生するソフトウェアにチェックを要することを表す符号が書かれているときにのみ、それを行うようにしても良い。そのようにしておけば、自由に配布可能なソフトウェアの場合には、識別番号無しで配布すれば、利用者は自由にコピーしてそれを使うことが可能になる。
【００３２】このようなＩＤにより、データの不正利用防止が可能になるが、ＩＤが書かれていないことは、すぐに認識できるものの、情報ソフトウェア１０に不正にＩＤが書き込まれている場合のことも考慮し、ＩＤは適当に振られるのではなく、ある規則に従って作成されるほうが良い。例えば、ＩＤが１０桁程度の整数からなるものとすると、下５桁と上５桁で分けて考え、上５桁の数Ｙは下５桁Ｘの数からある規則（関数ｆ）によって生成されるようにしておく。
【００３３】Ｙ＝ｆ（Ｘ）
例えば簡単には×に１２３（適当な数）を掛け、その下５桁をＹとするような方法であっても良い。関数が複雑なものであれば、それだけＩＤは不正に類推、生成しにくくなる。こうしておけば、ＩＤの生成規則を知らない限り、任意の数をＩＤとしてＨＤに書き込み、音楽データなどを不正使用することはできなくなる。再生を行うソフトウェアはこの生成規則からＩＤの正当性をチェックすることが可能である。
【００３４】尚、このような方式の場合、音楽再生用プログラム のようなデータを扱うためのソフトウェアは、ソフトウェアの利用を会員制等の形で、予め登録された会員にのみ配布しておく必要がある。このような会員には通常、会員番号が与えられることが多いので、この会員番号を利用してソフトウェアの不正利用を防止することも可能である。
【００３５】しかし上述の方法では、正当なＩＤが書き込まれたＨＤ同士でソフトウェアがコピーされた場合には、チェック用のプログラム を有した情報再生ソフトウェアでもＩＤのチェックは通過するため、ソフトウェアの不正利用が防げないという問題がある。これを防ぐために、以下に述べるような第２の方法がある。
【００３６】第４の実施の形態
そこで、ＨＤに記録されたソフトウェアにも、ＩＤに対応した何らかのデータを付加し、不正利用を防ぐ方法である。従ってＩＤに対応してソフトウェアの内容も一部書き足すことになるので、この方法では現在のようにＣＤ・ＲＯＭのような形で同じ内容のものを利用者に配布することはできなくなり、利用者の持つＨＤのＩＤ毎にソフトウェアの内容を書換える必要がある。
【００３７】しかし現在では、コンピュータネットワークを通じてデータをやりとりすることも可能になっているので、このような場合には、ここで述べるような方法で、ユーザーからソフトウェアの購入注文があった場合、そのユーザーの持つＩＤに従って、ソフトウェアを書換え、それを利用者に送ることもさほど困難性はない。このような処理はコンピュータ通信により行うことが可能である。
【００３８】第５の実施の形態
具体的な例として図４にネットワークによるソフトウェアの発注、転送システム の概念図を示して説明する。コンピュータネットワーク１６は今日隆盛なインターネットであり、利用者１７はパソコン９を利用してサービスセンター１８に必要とするソフトウェアを注文する。その際ハードディスク（記録媒体）８に付されたＩＤを連絡する。
【００３９】そして、サービスセンター１８では注文に応じた情報をデータベース１９から取り出し、連絡されたＩＤからソフトウェアデータへの付加情報を生成し、付加する。そしてそのソフトウェアを利用者１７に転送する。
【００４０】尚、ここでは利用者１７がＩＤをコンピュータネットワーク１６を通じてサービスセンター１８に送るようにしているが、サービスセンター１８では利用者１７のもつＨＤ８のＩＤを予め登録しておけば、利用

者１７が注文毎にＩＤをサービスセンターに送る必要は省略できる。
【００４１】ＰＣ上の音楽再生ソフトウェアでは、ＨＤ自体のＩＤとソフトウェアに書かれている符号（以降ＳＩＤと略す）を比較し、ＳＩＤとＩＤの対応が取れれば記録されたデータを再生するようにする。対応が取れなければ、データの再生を行わない。このようなしておけば、ＨＤ上のソフトウェアはそのＨＤがない限り再生ができず、ソフトウェアの不正利用防止ができる。
【００４２】ＳＩＤとＩＤの対応は、どのようなものでも良く、まったく同じものであっても構わないが、同じであると何らかの手段で不正利用がされやすくなるので、推測されにくくする方法として、例えば次のようなＩＤの構成法がある。即ち、適当な関数ｆ０，ｇ()を使い、次のような関係で生成できるようにする。
【００４３】ＳＩＤ＝ｆ（ＩＤ）又はＩＤ＝ｇ（ＳＩＤ）
関数ｆ()又はｇ()は図４で示すサービスセンター及びＰＣ側のデータ再生用ソフトウェアでは、どのような規則のものかわかっている必要があるのは無論のことである。そうでないと、サービスセンターでＩＤに対応したＳＩＤが生成できないし、再生用ソフトウェアではＳＩＤとＩＤの対応関係がわからないため、データの不正利用をチェックできない。
【００４４】上述のような方法でも、データ自体はそのままの形であるので、適当な方法でＳＩＤの含まれていないデータを抜き出し、それをコピーして不正利用されることも考えられる。
【００４５】第６の実施の形態
これを防ぐために、記録されるディジタルデータを符号化（暗号化）しておき、それを読み出すときに復号化し元のデータを取り出すようにする。ここでこの方法を判りやすく説明するために、ディジタルデータの暗号化方法について説明をする。
【００４６】暗号化は元の内容がわからないようにデータを変換する技術であり、具体的には元のデータを鍵データを使った関数（暗号アルゴリズム）で暗号データに変換するものである。図５に示すように、ディジタルデータの暗号化方法については２種類に分けることができる。
【００４７】図５（ａ）に示す共通鍵暗号化方式は暗号化、復号化の過程で同じ鍵データＫ（キーワード）を使うものであり、鍵データＫは通常秘密にする必要がある。図５（ｂ）に示す公開鍵暗号化方式は暗号化と復号化のときの鍵データに異なるものを使用するもので、この場合２つの鍵データＫｅ，Ｋｄの内一つは公開されていても、暗号安全性の面では問題はないとされており、復号操作は複雑なものの片方の鍵が個人的に秘密にされるため、本人認証や、データの正当性を保持するためにこれが使われることも多くなってきている。
【００４８】以上の暗号化方式を元に、ここでは暗号化鍵としてＩＤやＳＩＤを使って、データの不正利用を防止することを提案する。データの暗号化鍵としてＩＤ又はＳＩＤを利用すれば、データを暗号化して伝送することができる。
【００４９】第７の実施の形態
図６（ａ）は本発明の共通鍵暗号法を利用した転送方式の概念図であり、図６（ｂ）は公開鍵暗号法を利用した転送方式の概念図である。
【００５０】通常ＩＤはＨＤから読み出し可能であるので、利用者にＩＤがわかってしまうという意味では共通鍵暗号法でも公開鍵暗号法でもどちらも、データのセキュリティ上は問題がある。特に公開鍵暗号法はデータの正当性を利用者側でチェックする必要がある場合以外は、復号作業が複雑化しやすいので、この方法を使用する必要性は少ない。
【００５１】ＩＤが読めるとしても通常はデータが暗号化されていれば、利用者が簡単にデータの内容を読めるわけではないので、データの不正利用防止の効果はある。共通鍵暗号法でも、高度な安全性が求められる場合は別であるが、通常は鍵自体がわかっても、暗号アルゴリズムが公開されていなければ、簡単に元のデータが得られるわけではないので、ＩＤを鍵として使っても余り問題はない。又は、ＩＤは利用者が直接使う必要はないので、簡単な手段では利用者がＩＤを読み出せないようにできれば、データの不正利用の安全性はさらに高まる。
【００５２】ＩＤを読みにくくする手段としては、ＩＤ読み出しの手順を複雑化し、ＨＤ装置に対する単純なコマンドーつだけでは、ＩＤが読み出されないようにしておけば、利用者がＩＤを読み出すのは困難となる。この場合でも記録されたソフトウェアを利用するためのＰＣ上のソフトウェア（プログラム）では、予めその手順をプログラムしておけば、それによりＩＤを読み出すことができるので、実際のデータの読み出しには何ら問題はない。
【００５３】ＩＤを利用者が利用しにくくする手段として、ＩＤ自体を予め暗号化しておくことも有効である。ＩＤを暗号化してＨＤに記録しておけば、それを適当に書換えることも難しくなり、これもソフトウェアの不正利用防止には効果がある。但しこの場合、利用者が持つＩＤは予めサービスセンターで把握しておく必要がある。暗号化されたＩＤは、サービスセンターからソフトウェアに付随して送られる暗号鍵ＩＤＫで、復号化されるようにする。
【００５４】第８の実施の形態
図７にこの方法を利用したソフトウェアの暗号化、図８に復号化の過程を示す。即ち、サービスセンター側では、暗号化デコーダ２０ａにデータＳを供給して鍵データＳＩＤによって暗号化し、このデータにＩＤＫ付加デ

コーダ２１を付加し、暗号文データＣｓｉｄとして利用者のパソコン９に供給する。そしてパソコン９に付属されたハードディスク駆動装置（記録装置１）のＨＤ８に暗号文データＣｓｉｄを記録する

【００５５】暗号データの復号化は図８に示すごとく、暗号文データから成る音楽ソフトウェア２２をＨＤ８から読み出し、音楽再生ソフトウェア２３に供給する。同時に音楽ソフトウェア２３に含む鍵データＩＤＫを読み出し、ＩＤの復号化ソフトウェア２４に供給する。

【００５６】一方記録装置１からは暗号化されたＩＤ３が読み出され、ＩＤの復号化ソフトウェア２４に供給される。ＩＤの復号化ソフトウェア２４では鍵データＩＤＫにより、暗号化ＩＤの復号化が行われる。そして復号化されたＩＤ３を用いて音楽再生が復号化処理を含んで実行される。

【００５７】尚、この図８ではＩＤによるデータの復号化をＰＣ上のソフトウェアで行っているが、後述のようにハードウエアで行うことも考えられる。尚、図８のデータの復号化では図３に示した再生方式と対比し音楽データの復号化の例を示しているが、画像データやテキストデータの場合でも再生手順は同じであり、データの出力先がスピーカからディスプレーに変わるだけである。

【００５８】上記説明では暗号化されたデータの復号化は、ＰＣ上のＣＰＵでソフトウェアによって行われるものとして説明を行ったが、暗号化、復号化処理はその処理アルゴリズム によっては多大な計算量を必要とするものもあるため、復号化専用ハードウェアでその処理を行うことも良い。

【００５９】第９の実施の形態

ここではデータの復号処理に用いる復号用ハードウェア２５は、記録装置１に内蔵した形でもＰＣ９上に備えられた形でも構わない。

【００６０】暗号化された音楽データを再生する場合の処理システム ブロックを図９に示す。この例では、暗号化されたデータである音楽ソフトウェア２２を復号化するときに、まずＰＣ９上にロードされた音楽再生ソフトウェア１１で記録装置１のＩＤ３を認識し、それが正当なものであれば、記録装置１の復号用ハードウェア２５に対し、それが動作するよう適当なコマンド２５ａを出力する。

【００６１】その後暗号化されたデータを復号用ハードウエア２５を用いて復号化し、それをＰＣ９に転送しＰＣでデータ再生を行う。ＨＤ８上の暗号化されていないデータ１０ｂを利用する場合には、図９の点線矢印で示すように復号用ハードウェア２５を通さずにＰＣ９にデータ１０ｂを転送する。以上のようにすれば、ＰＣ９に復号化処理ソフトウェアを持つ必要はないので、複雑な復号化処理が必要な場合でもＣＰＵに余分な負荷がかかることを避けることができ、ＣＰＵに不必要に高性能なものを使う必要もなくなる。

【００６２】請求項９で述べた、利用者番号（以下ＵＩＤと略す）の利用はデータ再生ソフトウェアでＨＤ上のデータを再生するときに、ＩＤやＳＩＤなどの番号の他に利用者番号など別の番号をソフトウェア再生のための認証に利用するものである。前述のようにオンラインで有料データを転送する場合には、利用者番号等をサービスセンターに登録するのが普通であり、サービスセンターではこれを利用者名簿などに登録しておく。

【００６３】ばって、これをＩＤと共に利用してソフトウェアの不正利用防止を行うことが可能である。ＩＤを利用しないでＵＩＤだけをＩＤのように利用してソフトウェアの不正防止をすることも可能であるが（実際これは既に行われている方法である）、ＩＤと共に使うことで、データのセキュリティを高めることが可能である。

【００６４】ＵＩＤはデータ再生ソフトウェアを利用するたびに利用者が入力する方法でも良いが、予めＵＩＤを別のファイルに書き込んでおき、それをデータ再生ソフトウェアが読んで利用する方法もある。若干利用者にとっては面倒ではあるが、ソフトウェアを使用するときにＵＩＤを入力する方法がデータ保護の点では望ましいだろう。又は、サービスセンターがデータ再生ソフトウェアを利用者に提供するときに、そのソフトウェアにＵＩＤを組み込んでおく方法も考えられる。

【００６５】ＵＩＤはＩＤと同様に利用することが可能であり、例えば図１０のようにＵＩＤとＩＤを組み合わせて一つの新ＩＤとして利用し、データの正当性をチェックしたり、又は同様にＳＩＤと組み合わせたりして、データチェックのために利用することが可能である。ＩＤと組み合わせてＵＩＤをＳＩＤと同様に使えば、ＣＤ・ＲＯＭのような大量に同じ内容のものを記布する場合には（この場合ＳＩＤが使えない）、データの不正利用防止の効果は高い。

【００６６】又は、請求項１から請求項９で述べた方法を組み合わせて使い、データの不正利用を防ぐことも有効である。例えば、ＩＤ，ＳＩＤ，ＵＩＤといった識別番号を組み合わせて使い、それをお互いに利用してデータのチェックを行ったり、復号化処理を行ったりすることは様々な組み合わせ方法が考えられ、それによりデータの不正利用防止を一層強化することができる。

【００６７】以上の説明は、ＰＣなどのコンピュータで一般的に使われているＨＤ（ハードディスク）を例に行ったが、このようなデータの保護機構は他の記録装置、例えば磁気テープ記録装置やＭＯなどの光磁気記録装置などにも幅広く利用できる。

【００６８】又は記録装置に記録するソフトウェアとしても本文では音楽を演奏するためのディジタルデータを例にとって説明を行ったが、本発明で保護対象となるソフトウェアはこれに限らず、記録装置に記憶可能なディジタルデータであれば、画像データであって文章データであっても、コンピュータのプログラムであっても、同

様な手法で、ソフトウェアの不正使用防止を行うことができる。

【００６９】さらに、以上の説明はコンピュータの利用を前提として行ったが、このような記録装置の記録内容の保護方式は、例えばディジタル記録方式の音楽再生専用機の様な明示的にコンピュータを使ってはいない機器にも適用でき、一般的な記録保護方式として利用することも可能である。

【００７０】

【発明の効果】本発明を用いることにより、ハードディスク装置などの記録媒体に記録されたソフトウェアのコピーが難しくなり、不正コピーを防止できる。特にネットワークなどを通じて、ソフトウェアを配送する場合でもそれを利用できるのは機器の識別番号が特定できるものだけであり、ネットワーク上で配送途中のデータが盗まれたり、利用者によってコピーされても他のＰＣなどではそれを利用することができず、不正利用を未然に防止できる。その結果、各種ソフトウェアを提供する企業もネットワークなどを通じてソフトウェアを安心して利用者に配信可能になる。

【図面の簡単な説明】

【図１】　本発明のＩＤメモリーを備えた記録装置の回路ブロック図。

【図２】　本発明のＩＤを付した記録媒体の平面図。

【図３】　本発明のパーソナルコンピュータによる音楽再生システム ブロック図。

【図４】　ネットワークによるソフトウェアの発注、転送システム 概念図。

【図５】　暗号化方式のシステム 概念図。

【図６】　本発明の暗号方法を利用した転送方式。

【図７】　本発明のＩＤＫを付加した暗号データの転送方式概念図。

【図８】　音楽データを再生するためのＩＤの暗号化と復号化システム の概念図。

【図９】　本発明のハードウェアによるＩＤの復号化方式の機能ブロック図。

【図１０】　ＵＩＤとＩＤの組み合わせ原理図。

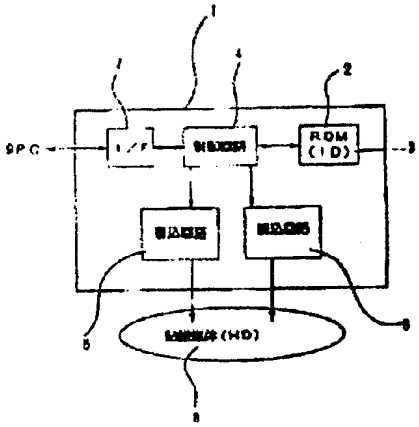
【図１１】　各種記録媒体とデスクトップ型ＰＣの接続を示す機構概念図。

【図１２】　ノート型ＰＣとＰＣＭＣＩＡ型ＨＤの接続を示す機構概念図。

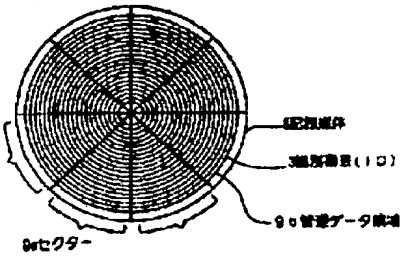
【符号の説明】

１…記録装置、２…識別番号（ＩＤ）メモリー、３…識別番号（ＩＤ）、４…制御回路、５…書込回路、６…読込回路、７…Ｉ／Ｆ、８…記録媒体、９…パソコン、９ａ…セクター、９ｂ…管理データ領域、１０…情報ソフトウェア、１１…情報（音楽）再生ソフトウェア、１２…メモリー、１３…ＣＰＵ、１４…音声処理回路、１５…スピーカ、１６…コンピュータネットワーク、１７…利用者、１８…サービスセンター、１９…データベース、２０…暗号データ、２０ａ…暗号化デコーダ、２１…ＩＤＫ付加デコーダ、２２…音楽ソフトウェア、２３…音楽再生ソフトウェア、２４…ＩＤの復号化ソフトウェア、２５…復号用ハードウェア、２６…動作指示プログラム、２６ａ…コマンド

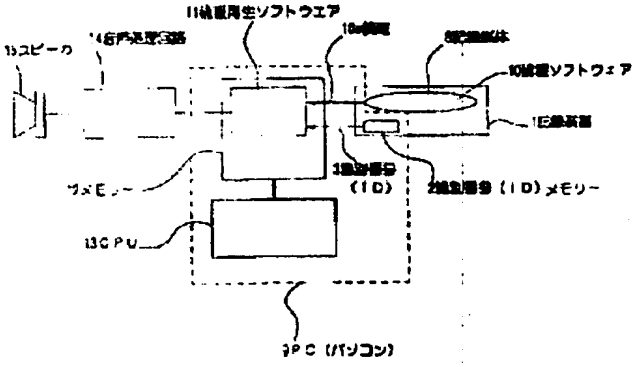
【図１】



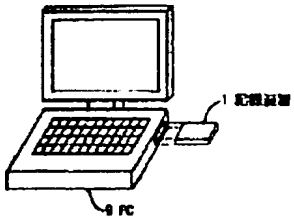
【図２】



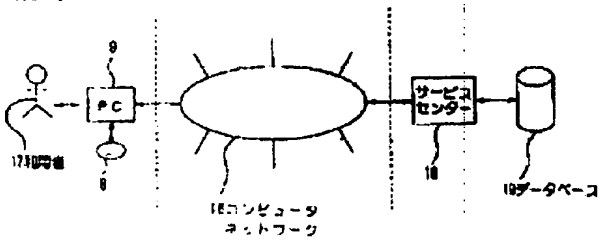
【図３】



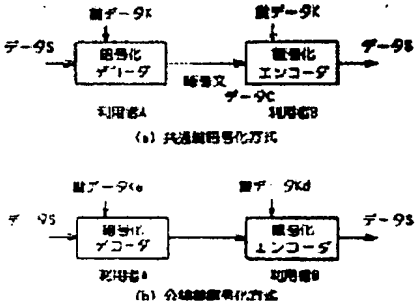
【図１２】



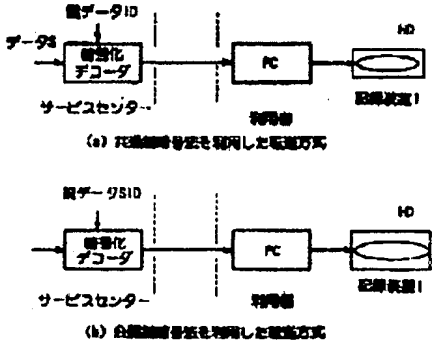
【図４】



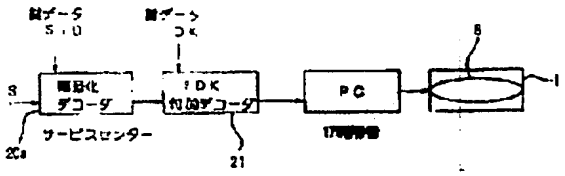
【図５】



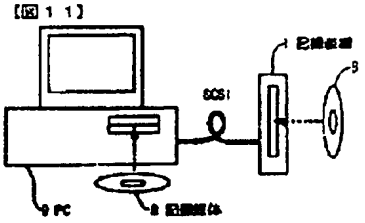
【図６】



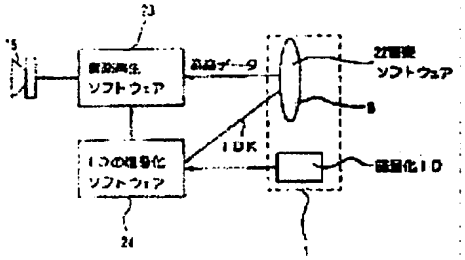
【図７】



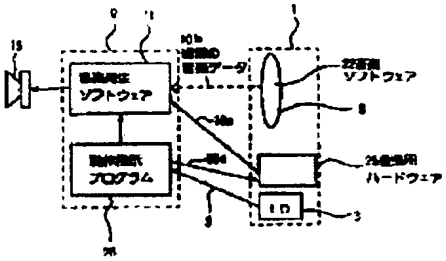
【図１１】



【図８】



【図９】



【図１０】